Firewalls

Syllabus definition:

“A firewall is a network security device that monitors incoming and outgoing network traffic and decided whether to allow or block specific traffic based on a defined set of security rules”

Firewalls

Markscheme points:

- acts as a barrier between a computer and external connections;
- monitors network traffic;
- makes sure that only authorised traffic is allowed;□
- prevents unauthorised access to the network (by checking IP/MAC address/packet content)
- inspects incoming/outgoing packets of data;
- to see if packets may be malicious;
- to see if packets may be allowed/disallowed by firewall settings/criteria;
- prevents unauthorised sending of data packets
- opens/closes ports as necessary;
- restricts use of certain services/ports;

Firewalls

A **network port** is a connection endpoint used to direct and sort network traffic

TCP and UDP use ports to direct network traffic, with the same sort of traffic always going to the same port - e.g. Port 80 is always used for HTTP activity; port 20 for FTP activity